

Docket No.: 62758-053

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of : Customer Number: 20277
Shingo HANE, et al. : Confirmation Number:
Serial No.: : Group Art Unit:
Filed: August 20, 2003 : Examiner:
For: ELECTRONIC DOCUMENT MANAGEMENT SYSTEM WITH THE USE OF
SIGNATURE TECHNIQUE CAPABLE OF MASKING

**CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT**

Mail Stop
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

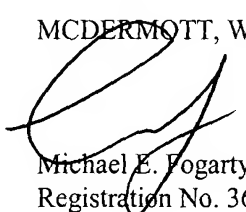
In accordance with the provisions of 35 U.S.C. 119, Applicants hereby claim the priority of:

Japanese Patent Application No. 2003-161505, filed June 6, 2003

A Certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY


Michael E. Fogarty
Registration No. 36,139

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 MEF:prg
Facsimile: (202) 756-8087
Date: August 20, 2003

02+20-000
HANE et al.
August 20, 2003

日 本 国 特 許 庁

JAPAN PATENT OFFICE *McDermott, Will & Emery*

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 6 月 6 日
Date of Application:

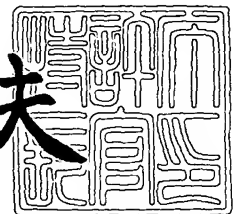
出 願 番 号 特 願 2 0 0 3 - 1 6 1 5 0 5
Application Number:
[ST. 10/C] : [J P 2 0 0 3 - 1 6 1 5 0 5]

出 願 人 株式会社日立製作所
Applicant(:

2 0 0 3 年 7 月 1 8 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 0 5 7 3 3 1

【書類名】 特許願

【整理番号】 K03001831A

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/21

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1099 番地 株式会社日立製作所 システム開発研究所内

【氏名】 羽根 慎吾

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1099 番地 株式会社日立製作所 システム開発研究所内

【氏名】 藤城 孝宏

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1099 番地 株式会社日立製作所 システム開発研究所内

【氏名】 鍛 忠司

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1099 番地 株式会社日立製作所 システム開発研究所内

【氏名】 熊谷 洋子

【発明者】

【住所又は居所】 東京都江東区新砂一丁目 6 番 27 号 株式会社日立製作所 公共システム事業部内

【氏名】 竹内 順一

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社日立製作所

【代理人】

【識別番号】 100075096

【弁理士】

【氏名又は名称】 作田 康夫

【手数料の表示】

【予納台帳番号】 013088

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 マスキング可能な署名技術を用いた電子文書管理システム

【特許請求の範囲】

【請求項 1】

電子文書を、任意または固定長の 2 つ以上の部分文書に分割したデータを作成するデータ作成装置と、

前記部分文書それぞれの正当性を確認するための情報を生成し、生成した複数の、前記部分文書の正当性を確認するための情報の集合体に対して署名を行う署名装置と、

前記署名の対象となった電子文書を、前記部分文書単位で、削除または変更するマスキング装置と、

前記マスキングされた電子文書の正当性を検証する検証装置とを備える電子文書管理システム。

【請求項 2】

請求項 1 に記載の電子文書管理システムであって、

前記検証装置は、

前記部分文書の正当性を確認するための情報の集合体を検証することにより、前記電子文書全体の正当性を確認し、

各々の前記部分文書の正当性を確認するための情報を検証することにより、検証対象となっている前記電子文書の部分文書の正当性を確認し、前記電子文書が部分的に削除または変更されているかどうかを確認する。

【請求項 3】

請求項 2 に記載の電子文書管理システムであって、

前記検証装置は、前記検証結果を表示部に表示することにより、検証者に、前記電子文書全体の正当性を保証しつつ、部分的に削除または変更されているかどうかを通知する。

【請求項 4】

請求項 1 に記載の電子文書管理システムであって、

前記データ作成装置は、前記部分文書の前および／または後に、区切り記号を

挿入することにより、前記分割を行う。

【請求項 5】

請求項 4 に記載の電子文書管理システムであって、
前記電子文書は、構造化言語を用いて作成された文書であり、前記部分文書は、前記構造化文書の構造化単位であり、前記区切り記号は、前記構造化言語のタグである。

【請求項 6】

請求項 2 に記載の電子文書管理システムであって、
部分文書の正当性を確認できる情報とは、ハッシュ関数を用いて生成した当該部分文書のハッシュ値である。

【請求項 7】

請求項 2 に記載の電子文書管理システムであって、
部分文書の正当性を確認できる情報とは、当該部分文書の署名である。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、デジタル署名技術とデジタル署名検証技術を用いた文書管理システムに関する。

【0002】

【従来の技術】

公開鍵暗号技術では、1 セットで 2 つの鍵が用いられる。一方の鍵で暗号化されたものはもう一方の鍵で復号化することが可能である。このとき、暗号化した鍵では暗号を解くことができず、対となるもう一方の鍵でのみ復号化が可能である。公開鍵暗号技術を利用する場合、一方の鍵は秘密鍵 (Private Key) として秘密に保管されてデジタル署名 (以下、署名という) の生成や暗号解読の際に使用される。もう一方の鍵は、公開鍵として公開され署名の検証や暗号化に用いられる。

【0003】

公開鍵暗号を署名に使用する場合、通常、はじめに署名対象となる電子文書を

SHA-1などのアルゴリズムを利用したハッシュ関数を用いてハッシュ値と呼ばれるダイジェスト値（特徴値ともいう）を求める。次にこのハッシュ値を秘密鍵で暗号化して署名値とする。

【0004】

署名の検証を行うには、公開鍵で署名値を復号化して電子文書のハッシュ値に戻す。次に電子文書のハッシュ値を計算して、この値と比較する。電子文書に改竄が無ければ二つのハッシュ値は一致する。改竄があれば電子文書から求めたハッシュ値が変化して二つの値は一致しない。この作業を行うことによって電子文書に改竄があったかどうかの判定が行える。

【0005】

この公開鍵を利用した署名方法の応用として、XML署名がある。XML署名における署名自体は対象となるデータのダイジェスト値を求め、秘密鍵で暗号化して行うことから、従来の技術と同様である。この署名法ではXMLタグを利用して、分割したデータなどへ署名を行うことができる。さらに、データの部分署名や多重署名などが行える。XML署名では、前述の署名がデータすべてに1つの署名を行うのに比べて、複雑な署名が行える。

【0006】

ほかの署名方法として分割署名方法がある。この署名方法では署名対象となる電子文書を分割し、分割した部分ごとに署名を行う。従来の署名方法では（例えば、特許文献1参照）、分割したデータに署名を行って保管する方法が記述されている。データを部分ごとに署名することで、部分ごとに独立して参照、編集することを可能にしている。

【0007】

【特許文献1】

特開 2001-167086号公報

【0008】

【発明が解決しようとする課題】

公的な機関が情報公開の請求にしたがって紙の文書を公開する際などに、プライバシー情報を含む場合にはその部分を黒く塗りつぶすなどのマスキング処理を

行い、文書を部分的に非公開とする。電子文書(以下、単に文書ともいう)においてもプライバシー情報の部分を除いた文書データを公開することができる。しかし、公開請求した文書に署名がされていた場合、課題が発生する。プライバシー保護のために過去に署名された電子文書を部分的にマスキングすると、文書の改竄を行ったことと同じになり過去の署名の有効性が失われてしまう。これはマスキングすることによって文書のハッシュ値が変化し、署名が保証するハッシュ値と対応がつかないからである。

【0009】

上記の課題を解決するための方法のひとつとして、再署名を行う方法と、上述の分割署名を行う方法がある。

【0010】

再署名の場合は、電子文書のマスキングを行った後で改めて署名を行い、修正時点での署名を施す。しかし、この方法だと文書作成時の署名が無効となってしまう、作成物の署名者とマスキングをする者が異なる場合や、署名時刻が一致しないことについて課題が発生する。

【0011】

特許文献1に記載された分割署名方法で署名されたデータにマスキングを行うと、マスキングを行った部分に施された署名が不正なものとなるが、分割した他の部分の署名は正当で検証に成功する。しかし、データ全体の対応関係に関してマスキング処理前からの正当性が保証できる署名がされていないので、分割した単位ごとにデータの順番などを変更しても、署名の検証で検出できないため、課題となる。

【0012】

【課題を解決するための手段】

本発明は、電子文書を、その公開の際に、部分的に非公開とする場合であっても、電子文書が作成された際に施された署名により、当該文書の正当性が検証できる技術を提供する。

【0013】

本発明のシステムは、署名の対象となる電子文書を、任意および／または固定

長の2つ以上の部分文書に分割する。この際、分割したXMLなど構造化言語のタグを用いて汎用性を持たせて分割するか、分割のために専用の区切りを挿入して分割を行う。この2つ以上の部分文書それぞれに対して、その正当性を確認するための情報を生成し、生成した正当性を確認するための情報の集合体に対して署名を行うことで電子文書に対する署名の効果を持たせ全体の正当性を確認する署名技術を用いる署名機能を備えている。

【0014】

また、この署名機能で署名された電子文書について、分割された部分文書単位に、削除または変更することによって電子文書の部分的な隠蔽（マスキング）を行うマスキング機能を備えている。また、この部分文書をマスキング単位という。

【0015】

さらに、この署名機能で署名された電子文書に於いて、正当性を確認するための情報の集合体に対する署名の検証によって電子文書全体の正当性を確認し、集合体に含まれるそれぞれの正当性を確認するための情報が、部分文書から生成する正当性を確認するための情報と比較し、等しい場合は電子文書が部分的に改竄されていないことを確認し、異なる場合は電子文書が部分的に隠蔽（マスキング）されていることを確認することによって、電子文書に対する正当性の検証を行う検証機能を備える。

【0016】

そして、上記正当性を確認するための情報は、ハッシュ関数を用いて部分文書（マスキング単位）から生成したハッシュ値か、または、部分文書の署名のいずれかを用いることができる。

【0017】

より具体的には、本発明のシステムは、その一態様において、署名後でもマスキングが可能となるように、電子文書を部分文書に分割したマスキング前データを作成するデータ作成装置と、部分文書から正当性を確認するための情報とその集合体に対する署名からなる署名関連データを作成する署名装置と、一つ以上の部分文書の削除または変更によりマスキングして、マスキング後データを作成す

るマスキング装置と、署名関連データでマスキング前データまたはマスキング後データを検証して電子文書の正当性を確認する検証機能とマスキング前データまたはマスキング後データと署名関連データを検証結果とともに表示するデータ表示機能とを備える検証装置と、からなる。

【0018】

【発明の実施の形態】

以下、図面を用いて本発明の実施の形態について説明する。

【0019】

図1は、本実施例における、マスキング可能な署名技術を用いた電子文書管理システム10の全体構成図である。

【0020】

図1のマスキング可能な署名技術を用いたシステム10はネットワーク20で繋がれた次の4つの装置で構成される。一つ目がデータ作成装置11で、元データ1から、署名後でもマスキングが可能となるマスキング前データ2を作成するデータ作成機能を持つデータ作成部21と、マスキング前データ2を表示するデータ表示機能を持つデータ表示部22を備える。

【0021】

二つ目が署名装置12で、マスキング前データ2へ署名して署名関連データ4を作成する署名機能を持つ署名部23と、署名関連データ4でマスキング前データ2を検証してデータの有効性を確認する署名検証機能をもつ署名検証部24と、マスキング前データ2と署名関連データ4を署名検証結果とともに表示するデータ表示機能を持つ表示部25を備える。

【0022】

三つ目がマスキング装置13で、マスキング前データ2またはマスキング後データ6の部分的な削除または変更によりマスキングして新たなマスキング後データ6を作成するマスキング機能を持つマスキング部26と、署名関連データ4でマスキング前データ2またはマスキング後データ6を検証してデータの有効性を確認する署名検証機能を持つ署名検証部27と、マスキング前データ2またはマスキング後データ6と署名関連データ4を署名検証結果とともに表示するデータ

表示機能を持つ表示部 28 を備える。

【0023】

四つ目が検証装置 14 で、マスキング前データ 2 またはマスキング後データ 6 と署名関連データ 4 を署名検証結果とともに表示するデータ表示機能を持つデータ表示部 29 と、署名関連データ 4 でマスキング前データ 2 またはマスキング後データ 6 を検証してデータの有効性を確認する検証機能を持つ検証部 30 を備える。

【0024】

上記データ作成装置 11、署名装置 12、マスキング装置 13、検証装置 14 は、基本ソフトウェア(オペレーティングシステムともいう)上でアプリケーションソフトウェアが動作する、少なくともマイクロプロセッサと、ハードディスクなどの二次記憶装置と、メモリと、キーボードやマウスなどの入力装置と、表示出力装置を備え、その他状況に合わせて G P U などのプロセッサや、着脱可能な記憶媒体の読み書き装置もしくは、ネットワークインターフェースなどの入出力装置を備えた一般的なコンピュータ上に実現される。

【0025】

データ作成装置 11 では基本ソフトウェア上で動作するアプリケーションを利用することによって、マスキング可能な署名技術で署名可能なデータ形式でデータを作成・編集・変換を行うことができる。データ作成装置 11 では、元データ 1 を編集または作成して、これを、署名後にマスキングが可能な形式であるマスキング前データ 2 に変換して表示する。このうちの、データの編集作成を行うのがデータ作成部 21 で、そのために必要な表示を行う部分が表示部 22 である。また、データ作成装置 11 で扱うデータは、基本ソフトウェアが提供する二次記憶装置や着脱可能な記憶媒体へのアクセス機能を利用することで適時読み込みと保存を行う。さらに、ネットワーク 20 を利用して署名装置 12 とデータの送受信を行う。

【0026】

署名装置 12 では基本ソフトウェア上で動作するアプリケーションを利用することによって、マスキング可能な署名技術で署名を行うことができる。署名装置

12では、データ作成装置11で作成されたマスキング前データ2に署名操作を行って署名関連データ4を作成し、次にマスキング前データ2とまとめて全データ3を作成して表示し、必要なら署名検証を行う。このうちの署名を行うのが署名部23で、署名検証を行うのが署名検証部24である。また、署名や検証結果の表示を行うのが表示部25である。また、署名装置12で扱うデータは、基本ソフトウェアが提供する二次記憶装置へのアクセス機能を利用することで適時読み込みと保存をする。さらに、ネットワーク20を利用してデータ作成装置11およびマスキング装置13とデータの送受信を行う。

【0027】

マスキング装置13では基本ソフトウェア上で動作するアプリケーションを利用することによって、マスキング可能な署名技術で署名を行ったデータを公開するために、非公開とすべき情報をマスキングする処理を行うことができる。マスキング装置13では、署名装置12で作成された全データ3のマスキング前データ2の必要箇所をマスキングしてマスキング後データ6を作成し、次に署名関連データ4とまとめて公開データ5を作成して表示し、必要なら署名検証を行う。このうちのマスキングを行うのがマスキング部26で、署名検証を行うのが署名検証部27である。また、マスキングや検証結果の表示を行うのが表示部28である。また、マスキング装置13で扱うデータは、基本ソフトウェアが提供する二次記憶装置へのアクセス機能を利用することで適時読み込みと保存をする。さらに、ネットワーク20を利用してデータ署名装置12および検証装置14とデータの送受信を行う。

【0028】

検証装置14では基本ソフトウェア上で動作するアプリケーションを利用することによって、マスキングが行われて公開されたデータを表示して確認することができる。マスキング装置13で作成された公開データ5の署名検証を行った上で表示する。また、検証装置14で扱うデータは、基本ソフトウェアが提供する二次記憶装置へのアクセス機能を利用することで適時読み込みと保存をする。さらに、ネットワーク20を利用してマスキング装置13とデータの送受信を行う。

。

【0029】

以下に説明する各処理は、上記ハードディスクまたはメモリに格納された一つ以上のプログラムを、基本ソフトウェアの管理のもと、マイクロプロセッサが読み出して実行することにより、各装置 11～14 上で実現されるものである。

【0030】

各プログラムは、あらかじめ、上記コンピュータのメモリ内に格納されていても良いし、必要なときに、当該コンピュータが利用可能な、着脱可能な記憶媒体または通信媒体(すなわち通信回線または通信回線上の搬送波)を介して、上記メモリに導入されてもよい。

【0031】

図2はシステムで扱うマスキング前データ2と署名関連データ4について詳細を示す。マスキング可能な署名の対象である元データ1は任意の文書データである。元データ1をマスキング前データ2に変換する際は、元データ1を複数のマスキング単位300に分割する。図2では例として4つのマスキング単位300a～300dに分割してあるが、分割は任意の箇所で任意の数だけ行うことができる。分割した箇所と署名データとの対応関係がわかるように、マスキング単位300の前後またはどちらか一方に、区切り301a～301dを作成して挿入する。

【0032】

一連のマスキング単位300と区切り301をまとめてマスキング前データ2として保存する。マスキング前データ2をマスキング可能な方法で署名する際は、署名関連データ4aもしくは署名関連データ4bを作成する2つの方法が選択できる。

【0033】

署名関連データ4aはマスキング前データ2を構成するマスキング単位300a～300dそれぞれのハッシュ値と対応情報302a～302dを求め、それらの集合体に対して署名値303aを求めることにより、作成する。署名関連データ4bはマスキング前データ2を構成するマスキング単位300a～300dそれぞれの署名値と対応情報304a～304dを求め、それらの集合体に対し

て署名値 303b を求めることにより、作成する。このマスキング前データ 2 と署名関連データ 4a または、マスキング前データ 2 と署名関連データ 4b をまとめて全データ 3 として保存を行う。

【0034】

図 3 はシステムで扱うマスキング後データ 6 について詳細を示す。全データ 3 のマスキング前データ 2 のマスキング単位 300a ~ 300d のうちマスキングが必要な部分に対して、データの消去または変更を行い、マスキング後データ 6 を作成する。例として、マスキング単位 300b を 300b' として変更してある。署名関連データ 4 とともに公開データ 5 として保存する。

【0035】

署名の検証を行うには、署名関連データ 4a または 4b をもちいて検証する。はじめに署名値 303a または 303b の署名を検証し、検証が失敗すれば署名対象となったマスキング前データ 2 またはマスキング後データ 6 全体の変更があったとする。署名値 303a または 303b の署名検証が成功した場合は、ハッシュ値と対応情報 302 または、署名値と対応情報 304 を用いてマスキング単位 300 ごとに検証を行う。ハッシュ値と対応情報 302 で検証を行う場合は、対応するマスキング単位 300 のハッシュ値とハッシュ値と対応情報 302 のハッシュ値と比較を行い、同じなら検証の成功、異なるならば検証失敗となる。署名値と対応情報 304 で検証を行う場合は、対応するマスキング単位 300 を署名値と対応情報 302 の署名値で検証を行いう。マスキング単位 300 の検証が成功した場合は、文書に署名がされてから改ざんがされていなかったことがわかる。一方、検証が失敗した場合は、そのマスキング単位 300 がマスキングされたか改ざんされたことがわかる。

【0036】

図 4 は、データ作成装置 11 で使用する、データ作成部 21 のフローチャート図である。各ステップにおける動作を記述するが、すべてのステップの任意のタイミングで、ネットワーク 20 や入出力装置を利用してデータの保存と読み込みを行うことができる。

【0037】

ステップ 111 に於いてデータ作成部 21 で使用される元データ 1 があるかどうか判定を行う。元となるデータがある場合はステップ 113 に進む。元となるデータが無い場合はデータを作成または編集するためにステップ 112 に進む。

【0038】

ステップ 112 に於いてマスキング可能な署名形式で署名可能なデータである、マスキング前データ 2 の元データ 1 を作成する。データを外部から入力して、元データ 1 として用いることもできる。元データ 1 を作成したらステップ 113 に進む。

【0039】

ステップ 113 では元データのデータ形式を判定する。元データがマークアップ言語など構造化されたデータである場合、ステップ 114 へ進み、そうでない場合はステップ 115 へ進む。

【0040】

ステップ 114 では、マークアップ言語などで構造化されたデータは、構造化のタグなどを区切りとして、そのままマスキング前データ 2 として使用することができるので、更なる分割の必要が無い場合がある。そのため、小さなマスキング単位 300 への分割を行うかどうかの選択が行い、分割を行う場合はステップ 115 へ進み、必要が無い場合はデータ作成部 21 での処理を終了する。

【0041】

ステップ 115 においては、元データ 1 をマスキング単位 300 となる小さな部分に区切って分割を行い、ステップ 116 に進む。分割方法は固定長・可変長の任意の選択が可能である。

【0042】

ステップ 116 では、マスキング単位 300 に分割した元データ 1 の区切りの場所がわかるようにするための分割情報をマークアップ言語のタグまたはその他区切りとなるデータを使用して作成する。分割情報を作成したらステップ 117 に進む。

【0043】

ステップ 117 では、分割情報を元データ 1 に挿入してマスキング前データ 2

を作成し、データ作成部 21 におけるステップを終了する。

【0044】

図 5 は、データ作成装置 11 で使用する、表示部 22 のフローチャート図である。各ステップにおける動作を記述するが、すべてのステップの任意のタイミングで、ネットワーク 20 や入出力装置を利用してデータの保存と読み込みを行うことができる。

【0045】

ステップ 121 では表示するデータが元データ 1 かマスキング前データ 2 であるか判断する。マスキング前データ 2 であった場合はステップ 122 へ進み、マスキング前データ 2 でなく元データ 1 であった場合はステップ 123 に進む。

【0046】

ステップ 122 では、表示するマスキング前データ 2 の区切りを検出し、ステップ 123 に進む。

【0047】

ステップ 123 は、元データ 1 のマスキング単位 300 が視覚的にわかるように区切りを入れてマスキング前データ 2 またはマスキング後データ 6 を表示し、表示部 22 におけるステップを終了する。

【0048】

図 6 は、署名装置 12 で使用する、署名部 23 のフローチャート図である。各ステップにおける動作を記述するが、すべてのステップの任意のタイミングで、ネットワーク 20 や入出力装置を利用してデータの保存と読み込みを行うことができる。

【0049】

ステップ 131 は、マスキング前データ 2 へ署名を行う範囲を 1 つまたは複数個の区切りで区切られた部分（以下、マスキング単位 300 という）を選択する。

【0050】

ステップ 132 は、ステップ 131 で選択した範囲に対しての署名技術を選択する。署名技術としては、マスキング単位 300 ごとにハッシュ値のみを求める

方法と、マスキング単位 300 ごとに署名を行う方法がある。ハッシュ値を求める場合はステップ 133 に進み、署名を行う場合はステップ 134 に進む。

【0051】

ステップ 133 は、ステップ 131 で選択した範囲のマスキング単位 300 すべてに対してハッシュ値を求め、ステップ 134 に進む。

【0052】

ステップ 134 は、ステップ 131 で選択した範囲のマスキング単位 300 すべてに対して署名し、署名値を求める。署名値を求めステップ 135 に進む。

【0053】

ステップ 135 は、ステップ 133 またはステップ 134 で求めたハッシュ値または署名値の集合体を作成し、ステップ 136 に進む。

【0054】

ステップ 136 は、ステップ 135 で作成した集合体に対して署名を行う。

【0055】

ステップ 137 は、ステップ 135 で求めた集合体と、ステップ 136 で求めた署名値が含まれる、署名関連データ 4 を作成する。マスキング前データ 2 と署名関連データ 4 とをまとめて全データ 3 として保管し、署名部 23 におけるステップを終了する。

【0056】

署名装置 12 の署名検証部 24 の動作を、図 7 のフローチャートを用いて説明する。各ステップにおける動作を記述するが、すべてのステップの任意のタイミングで、ネットワーク 20 や入出力装置を利用してデータの保存と読み込みを行うことができる。

【0057】

ステップ 141 は、全データ 3 または公開データ 5 に含まれる署名関連データ 4 におけるハッシュ値または署名値の集合体に対する署名の検証を行う。署名検証が成功すればハッシュ値または署名値の集合体の正当性が保証され、全データ 3 に含まれるマスキング前データ 2 の検証が行える。署名検証に失敗すると、ハッシュ値または署名値の集合体の正当性が保証できないため、マスキング前デー

タ 2 の正当性も保証できない。検証作業を行った後ステップ 1 4 2 に進む。

【0058】

ステップ 1 4 2 は、ステップ 1 4 1 で行った署名検証が成功したかどうか判別し、成功した場合はステップ 1 4 3 に進み、失敗した場合はステップ 1 4 7 に進む。

【0059】

ステップ 1 4 3 は、署名関連データ 4 から、署名技術がマスキング単位 3 0 0 に対するハッシュ値を用いる場合か署名を行う場合かの判別を行う。ハッシュ値を用いる方法の場合、ステップ 1 4 4 に進み、署名を行う場合は 1 4 6 に進む。

【0060】

ステップ 1 4 4 では、ステップ 1 4 3 と同様に、マスキング前データ 2 のマスキング単位 3 0 0 すべてに対してハッシュ値を求め、ステップ 1 4 5 に進む。

【0061】

ステップ 1 4 5 は、ステップ 1 4 2 の署名検証で保証されたハッシュ値と、ステップ 1 4 4 で求めたハッシュ値の比較によって、マスキング単位 3 0 0 の検証を行う。2 つのハッシュ値が等しければ、対応するマスキング単位 3 0 0 に対してマスキングや改竄が行われておらず、正当性が保証される。一方、2 つのハッシュ値が異なれば、対応するマスキング単位 3 0 0 に対してマスキングや改竄が行われていることになる。検証後、ステップ 1 4 7 に進む。

【0062】

ステップ 1 4 6 では、ステップ 1 4 2 の署名検証で保証された署名値を用いて、対応するハッシュ単位の署名検証を行う。署名検証が成功すれば、対応するマスキング単位 3 0 0 に対してマスキングや改竄が行われておらず、正当性が保証される。一方、署名検証が成功すれば、対応するマスキング単位 3 0 0 に対してマスキングや改竄が行われていることになる。検証後、ステップ 1 4 7 に進む。

【0063】

ステップ 1 4 7 では、ステップ 1 4 5 またはステップ 1 4 6 でのマスキング単位 3 0 0 に対する検証をまとめて結果を作成する。

【0064】

署名装置 12 の表示部 25 の動作を図 8 のフローチャートを用いて説明する。各ステップにおける動作を記述するが、すべてのステップの任意のタイミングで、ネットワーク 20 や入出力装置を利用してデータの保存と読み込みを行うことができる。

【0065】

ステップ 151 では表示するマスキング前データ 2 に署名関連データがあり、署名が行われているか判断する。署名が行われていた場合はステップ 152 へ進み、署名が行われていない場合はステップ 153 に進む。

【0066】

ステップ 152 では、表示するマスキング前データ 2 の署名を検証するために署名検証部 24 を使用して署名の検証を行い、署名の検証結果を得る。その後、ステップ 153 に進む。

【0067】

ステップ 153 は、元データ 1 のマスキング単位 300 が視覚的にわかるように区切りを入れてマスキング前データ 2 を表示し、なおかつ、署名の検証が成功した箇所が視覚的にわかるように表示色を変えて表示し、表示部 25 におけるステップを終了する。

【0068】

図 9 は、マスキング装置 13 のマスキング部 26 のフローチャート図である。各ステップにおける動作を記述するが、すべてのステップの任意のタイミングで、ネットワーク 20 や入出力装置を利用してデータの保存と読み込みを行うことができる。

【0069】

ステップ 161 は、全データ 3 に含まれるマスキング前データ 2 のマスキングを行うマスキング単位 300 を選択し、ステップ 162 に進む。

【0070】

ステップ 162 は、ステップ 161 で選択した範囲を変更・隠蔽してマスキングを行う。マスキングを行うには選択箇所のデータを削除すればよいが、「マスキングが行われた」などのデータと置き換えることも可能である。ステップ 16

3に進む。

【0071】

ステップ163は、ステップ161およびステップ162を繰り返すための判断を行うステップで、ステップ162でマスキングを行ったマスキング単位300以外にも、マスキングを行う箇所がある場合、繰り返しを選択してステップ161に戻る。マスキングを行うマスキング単位300がこれ以上ない場合はステップ164に進む。

【0072】

ステップ164では、ステップ164までに行われたマスキング単位300を反映し、マスキング後データ6を作成する。マスキング後データ6と署名関連データ4をまとめて公開データ5として保管し、マスキング部25におけるステップを終了する。

【0073】

マスキング装置13の署名検証部27の動作を、図7のフローチャートを用いて説明する。各ステップにおける動作を記述するが、すべてのステップの任意のタイミングで、ネットワーク20や入出力装置を利用してデータの保存と読み込みを行うことができる。

【0074】

ステップ141は、全データ3または公開データ5に含まれる署名関連データ4におけるハッシュ値または署名値の集合体に対する署名の検証を行う。署名検証が成功すればハッシュ値または署名値の集合体の正当性が保証され、全データ3のマスキング前データ2または公開データ5のマスキング後データ6の検証が行える。署名検証に失敗すると、ハッシュ値または署名値の集合体の正当性が保証できないため、マスキング前データ2またはマスキング後データ6の正当性も保証できない。検証作業を行った後ステップ142に進む。

【0075】

ステップ142は、ステップ141で行った署名検証が成功したかどうか判別し、成功した場合はステップ143に進み、失敗した場合はステップ147に進む。

【0076】

ステップ143は、署名関連データ4から、署名技術がマスキング単位300に対するハッシュ値を用いる場合か署名を行う場合かの判別を行う。ハッシュ値を用いる方法の場合、ステップ144に進み、署名を行う場合は146に進む。

【0077】

ステップ144では、ステップ133と同様に、マスキング前データ2またはマスキング後データ6のマスキング単位300すべてに対してハッシュ値を求め、ステップ145に進む

ステップ145は、ステップ142の署名検証で保証されたハッシュ値と、ステップ144で求めたハッシュ値の比較によって、マスキング単位300の検証を行う。2つのハッシュ値が等しければ、対応するマスキング単位300に対してマスキングや改竄が行われておらず、正当性が保証される。一方、2つのハッシュ値が異なれば、対応するマスキング単位300に対してマスキングや改竄が行われていることになる。検証後ステップ147に進む。

【0078】

ステップ146では、ステップ142の署名検証で保証された署名値を用いて、対応するハッシュ単位の署名検証を行う。署名検証が成功すれば、対応するマスキング単位300に対してマスキングや改竄が行われておらず、正当性が保証される。一方、署名検証が成功すれば、対応するマスキング単位300に対してマスキングや改竄が行われていることになる。検証後ステップ147に進む。

【0079】

ステップ147では、ステップ145またはステップ146でのマスキング単位300に対する検証をまとめて結果を作成する。

【0080】

マスキング装置13の表示部28の動作を図8のフローチャートを用いて説明する。各ステップにおける動作を記述するが、すべてのステップの任意のタイミングで、ネットワーク20や入出力装置を利用してデータの保存と読み込みを行うことができる。

【0081】

ステップ151では表示する全データ3のマスクング前データ2または公開データ5のマスクング後データ6に署名関連データ4があり、署名が行われているか確認する。署名が行われていた場合はステップ152へ進み、署名が行われていない場合はステップ153に進む。

【0082】

ステップ152では、表示する全データ3のマスクング前データ2または公開データ5のマスクング後データ6の署名を検証するために署名検証部27を使用して署名の検証を行い、署名の検証結果を得る。その後、ステップ153に進む。

【0083】

ステップ153は、元データ1のマスクング単位300が視覚的にわかるように区切りを入れて全データ3のマスクング前データ2または公開データ5のマスクング後データ6を表示し、なおかつ、署名の検証が成功した箇所とマスクングがされていた箇所が視覚的にわかるように表示色を変えて表示し、表示部28におけるステップを終了する。

【0084】

検証装置14の検証部30の動作を、図7のフローチャートを用いて説明する。各ステップにおける動作を記述するが、すべてのステップの任意のタイミングで、ネットワーク20や入出力装置を利用してデータの保存と読み込みを行うことができる。

【0085】

ステップ141は、公開データ5に含まれる署名関連データ4におけるハッシュ値または署名値の集合体に対する署名の検証を行う。署名検証が成功すればハッシュ値または署名値の集合体の正当性が保証され、全データ3または公開データ5に含まれるマスクング後データ6の検証が行える。署名検証に失敗すると、ハッシュ値または署名値の集合体の正当性が保証できないため、マスクング後データ6の正当性も保証できない。検証作業を行った後ステップ142に進む。

【0086】

ステップ142は、ステップ141で行った署名検証が成功したかどうか判別

し、成功した場合はステップ143に進み、失敗した場合はステップ147に進む。

【0087】

ステップ143は、署名関連データ4から、署名技術がマスキング単位300に対するハッシュ値を用いる場合か署名を行う場合かの判別を行う。ハッシュ値を用いる方法の場合、ステップ144に進み、署名を行う場合は146に進む。

【0088】

ステップ144では、ステップ143と同様に、マスキング後データ6のマスキング単位300すべてに対してハッシュ値を求め、ステップ145に進む

ステップ145は、ステップ142の署名検証で保証されたハッシュ値と、ステップ144で求めたハッシュ値の比較によって、マスキング単位300の検証を行う。2つのハッシュ値が等しければ、対応するマスキング単位300に対してマスキングや改竄が行われておらず、正当性が保証される。一方、2つのハッシュ値が異なれば、対応するマスキング単位300に対してマスキングや改竄が行われていることになる。検証後ステップ147に進む。

【0089】

ステップ146では、ステップ142の署名検証で保証された署名値を用いて、対応するハッシュ単位の署名検証を行う。署名検証が成功すれば、対応するマスキング単位300に対してマスキングや改竄が行われておらず、正当性が保証される。一方、署名検証が成功すれば、対応するマスキング単位300に対してマスキングや改竄が行われていることになる。検証後ステップ147に進む。

【0090】

ステップ147では、ステップ145またはステップ146でのマスキング単位300に対する検証をまとめて結果を作成する。

【0091】

検証装置14の表示部29の動作を、図8のフローチャートを用いて説明する。各ステップにおける動作を記述するが、すべてのステップの任意のタイミングで、ネットワーク20や入出力装置を利用してデータの保存と読み込みを行うことができる。

【0092】

ステップ151では表示するマスキング後データ6に署名関連データがあり、署名が行われているか確認する。署名が行われていた場合はステップ152へ進み、署名が行われていない場合はステップ153に進む。

【0093】

ステップ152では、表示するマスキング後データ6の署名を検証するために検証部30を使用して署名の検証を行い、署名の検証結果を得る。その後、ステップ153に進む。

【0094】

ステップ153は、元データ1のマスキング単位300が視覚的にわかるように区切りを入れてマスキング後データ6を表示し、なおかつ、署名がされていた場合は、署名の検証が成功した箇所とマスキングがされていた箇所が視覚的にわかるように表示色を変えて表示し、表示部29におけるステップを終了する。

【0095】

このように、本実施例のシステムでは、署名を行った時の署名が有効な状態で電子文書の一部分をマスキングすることが可能であり、さらに、マスキングを行った場所が特定できる。この特徴を利用して、署名つき文書を公開する際の問題に対応することができる。図14の電子文書管理システム10では、公的機関の担当官である電子文書作成者201がデータ作成装置11でマスキング前データ2を作成、保存し、ネットワーク20を通じて電子文書責任者202に渡す。公的機関の処分権者である電子文書責任者202は署名装置12でマスキング前データ2にマスキング後も署名可能な署名技術で署名を行い、全データ3として保管する。そして、情報公開法によって一般の公開要求者から保管してある全データ3の公開の要求があり、プライバシー情報の保護などの目的で全データ3をマスキング（部分的に隠蔽）することが必要な場合、公的機関の情報公開窓口の担当者である公開者はマスキング装置13で保管してあった全データ3をネットワーク20経由で読み込み、このうち必要な箇所をマスキングして公開データ5を作成して公開要求者にネットワーク20を通じて公開する。公開要求者は受け取った公開データ5を検証装置14で表示し、内容の確認を行う。

【0096】

なお、本実施例の電子文書管理システム10の構成は、上記実施例に限られるものではなく、たとえば、各装置内の各処理部単位に異なる装置上に実現されて、互いにネットワークで接続されても良い。

【0097】**【発明の効果】**

本発明によれば、管理する電子文書に対して、署名後の電子文書の部分的な隠蔽および／または変更によるマスキングを可能にしつつ、正当性の保証と、マスキングをした箇所の検出を行うことができる。

【図面の簡単な説明】**【図1】**

実施形態における、署名付き電子文書管理システムのシステム構成を示す図である。

【図2】

実施形態における、マスキング前データ2と署名関連データ4の図である。

【図3】

実施形態における、マスキング後データ6の図である。

【図4】

実施形態における、データ作成装置11のデータ作成部21の動作フロー図である。

【図5】

実施形態における、データ作成装置11の表示部22の動作フロー図である。

【図6】

実施形態における、署名装置12の署名部23の動作フロー図である。

【図7】

実施形態における、署名装置12の署名検証部24とマスキング装置13の署名検証部27と検証装置14の検証部30の動作フロー図である。

【図8】

実施形態における、署名装置12の表示部25と、マスキング装置13の表示

部 28 と、検証装置 14 の表示部 29 の動作フロー図である。

【図 9】

実施形態における、マスキング装置 13 のマスキング部 26 の動作フロー図である。

【図 10】

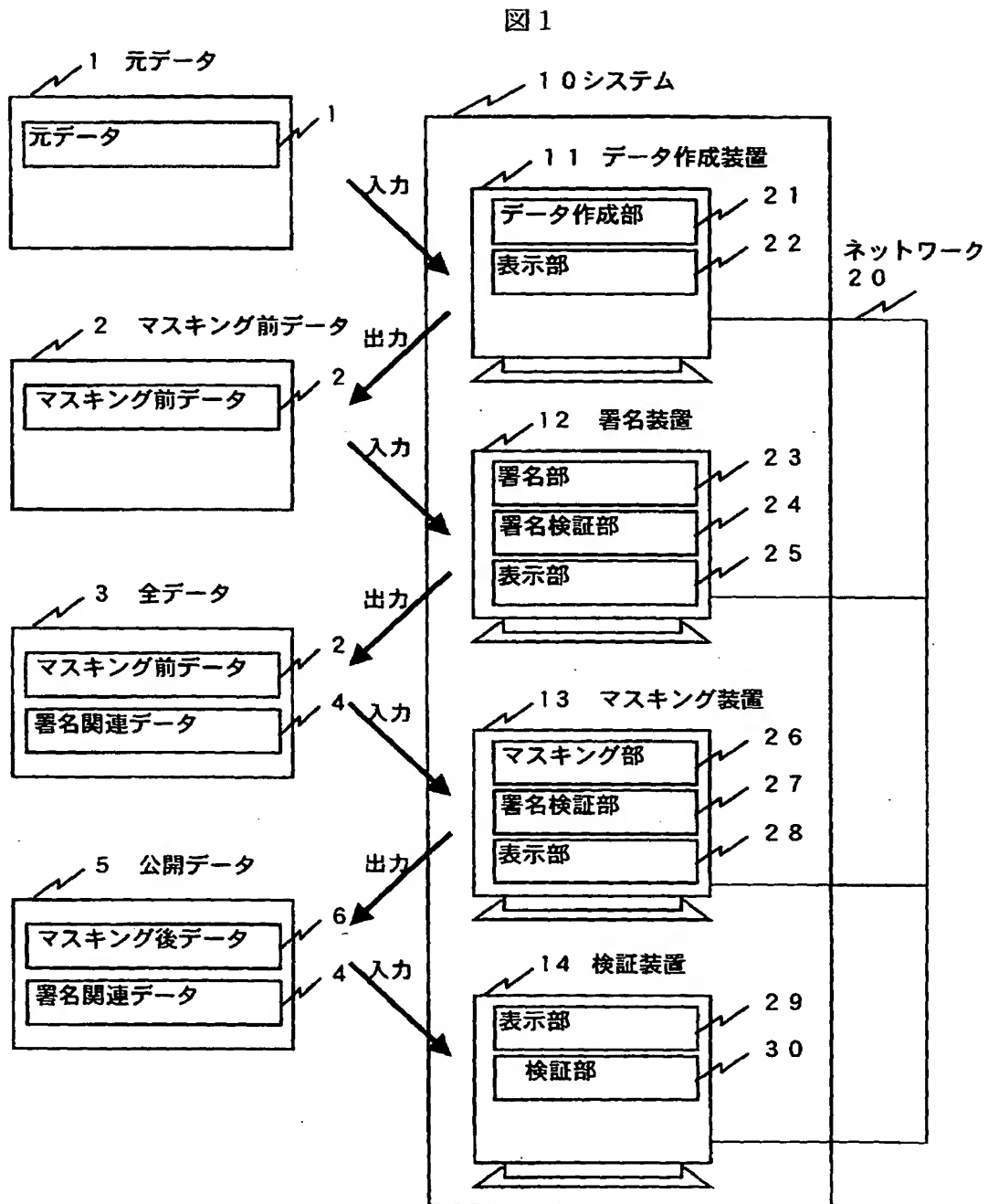
実施形態における、署名付き電子文書管理システムの使用例を示す図である。

【符号の説明】

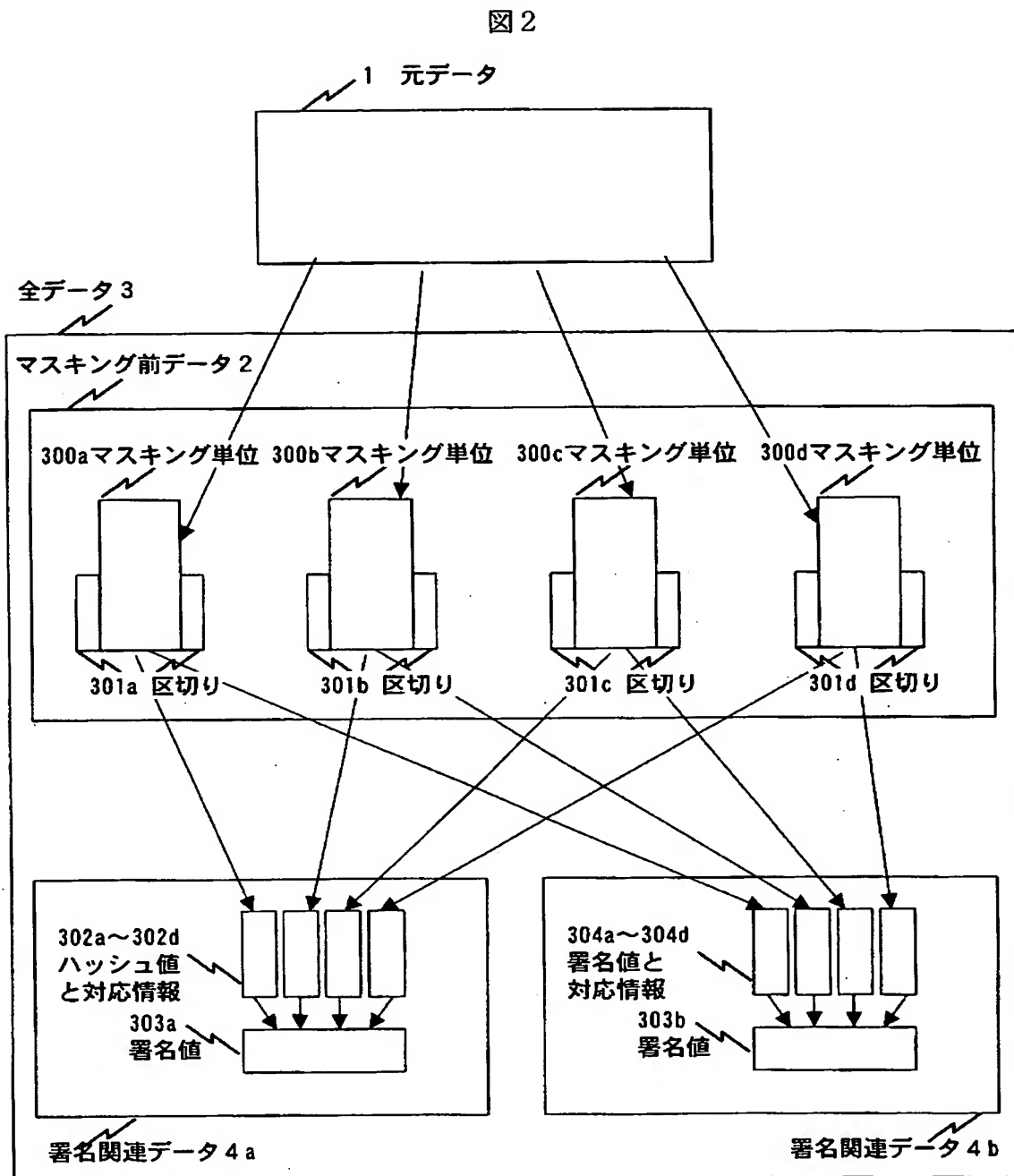
1…元データ、2…マスキング前データ、3…全データ、4…署名関連データ、4a…署名関連データ、4b…署名関連データ、5…公開データ、6…マスキング後データ、10…システム、11…データ作成装置、12…署名装置、13…マスキング装置、14…検証装置、20…ネットワーク、21…データ作成部、22…表示部、23…署名部、24…署名検証部、25…表示部、26…マスキング部、27…署名検証部、28…表示部、29…表示部、30…検証部、201…電子文書作成者、202…電子文書責任者、203…公開者、204…公開要求者、300…マスキング単位、300a…マスキング単位、300b…マスキング単位、300b'…マスキング単位、300c…マスキング単位、300d…マスキング単位、301…区切り、301a…区切り、301b…区切り、301c…区切り、301d…区切り、302…ハッシュ値と対応情報、302a…ハッシュ値と対応情報、302b…ハッシュ値と対応情報、302c…ハッシュ値と対応情報、302d…ハッシュ値と対応情報、303…署名値、303a…署名値、303b…署名値、304…署名値と対応情報、304a…署名値と対応情報、304b…署名値と対応情報、304c…署名値と対応情報、304d…署名値と対応情報。

【書類名】 図面

【図1】

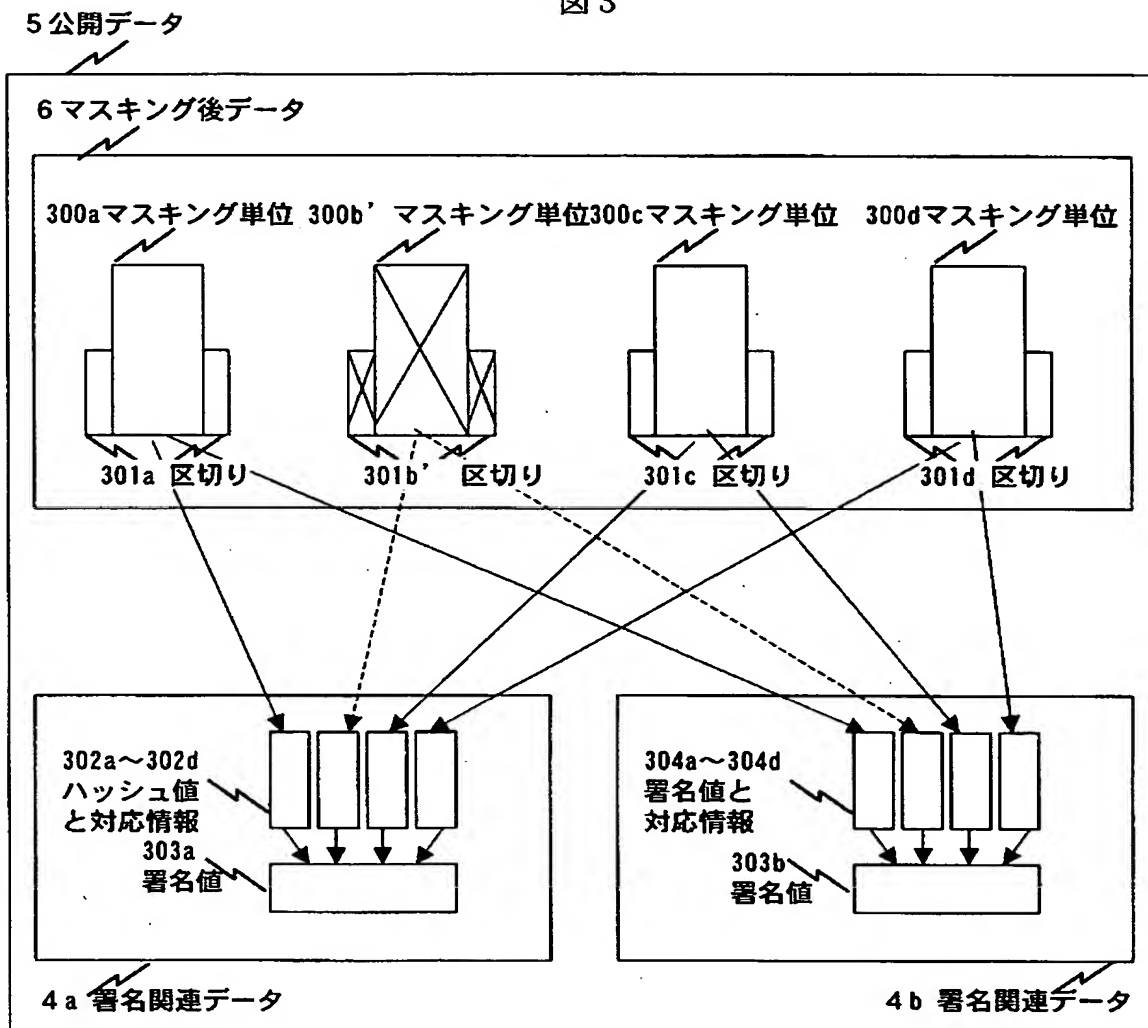


【図 2】



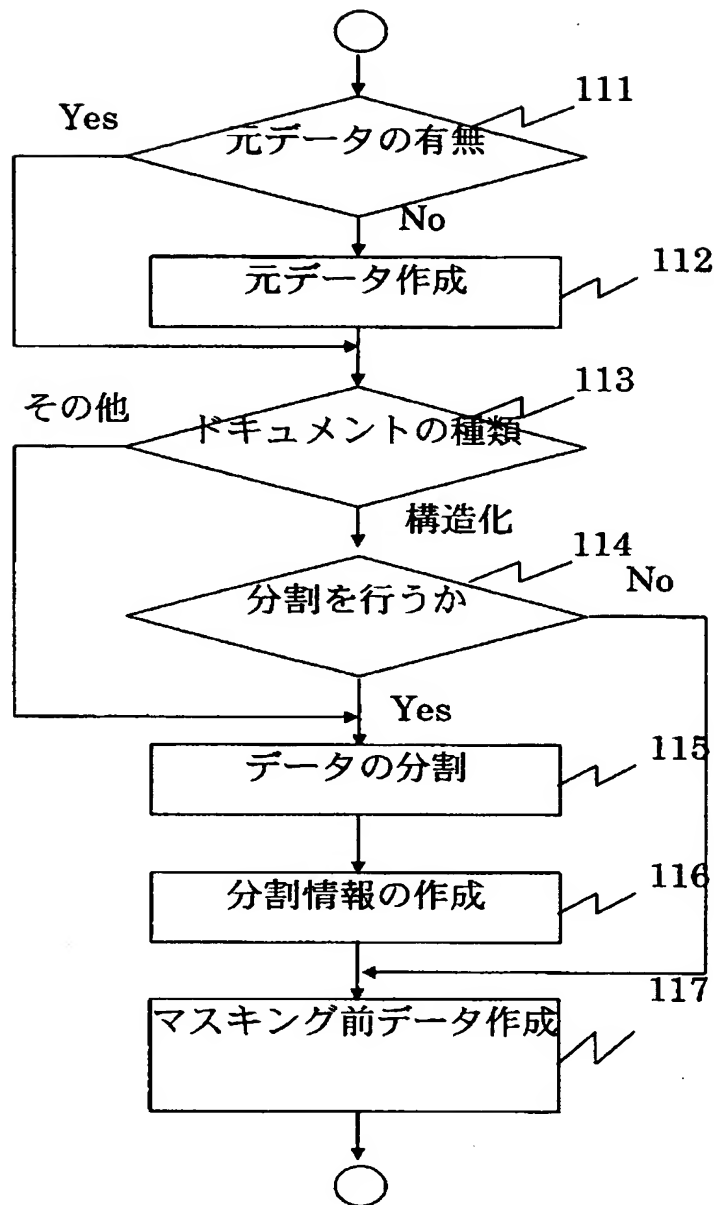
【図 3】

図 3



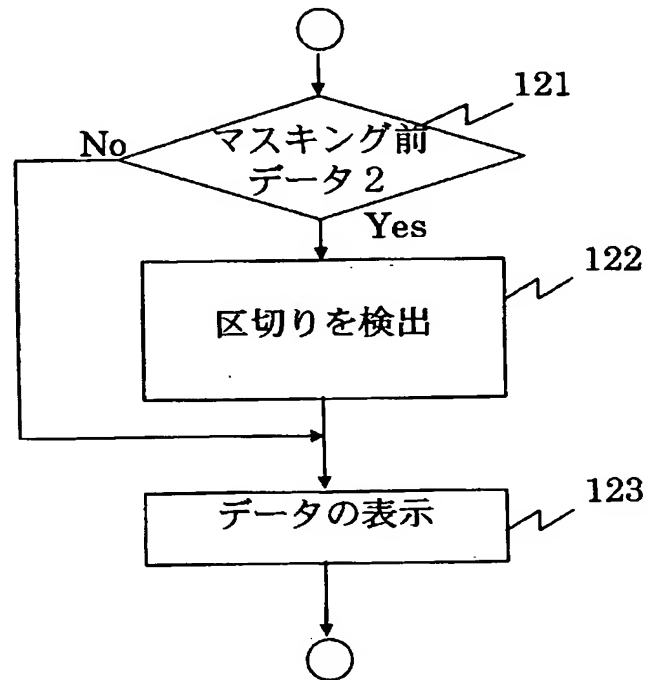
【図 4】

図 4



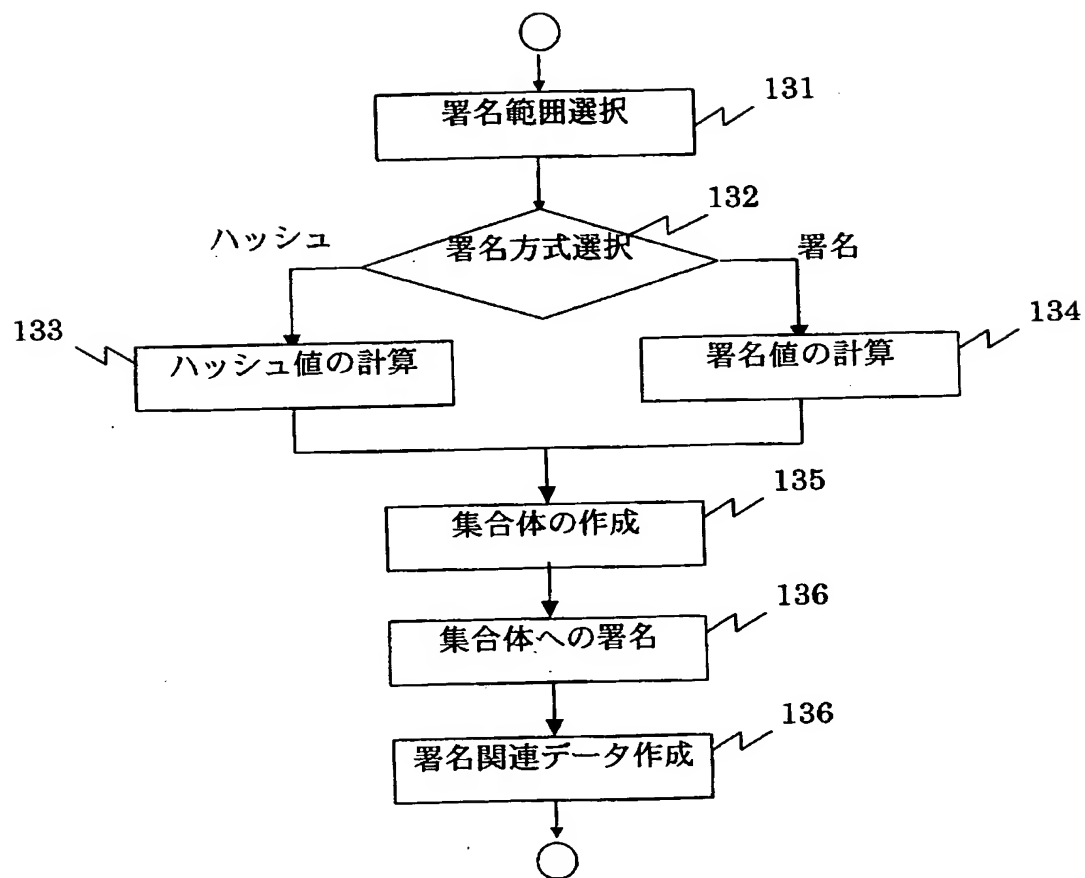
【図 5】

図 5



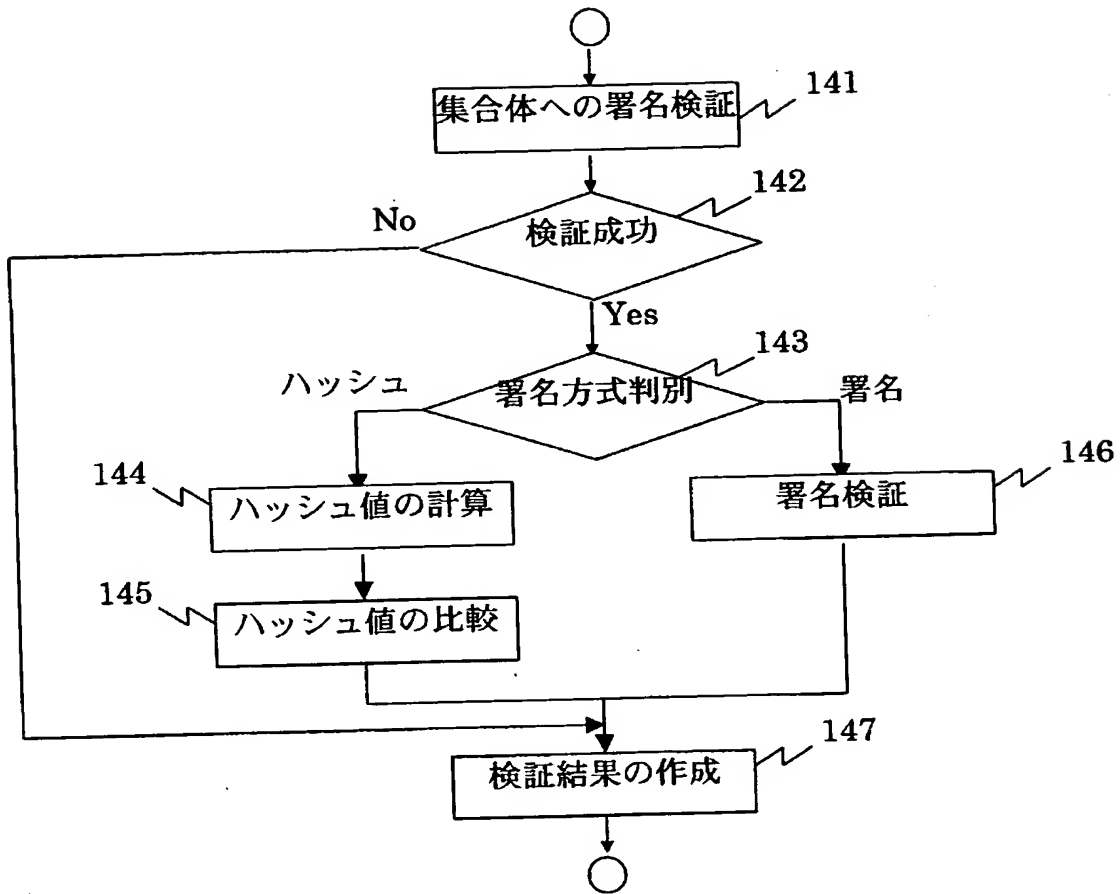
【図 6】

図 6



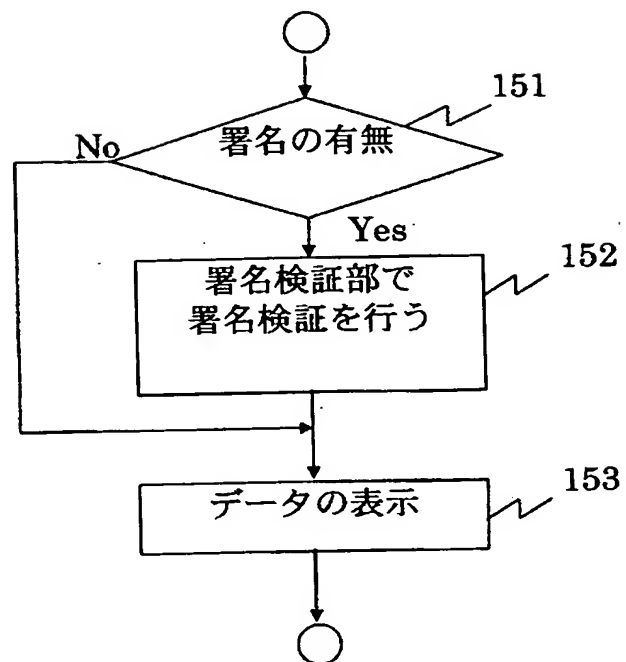
【図 7】

図 7



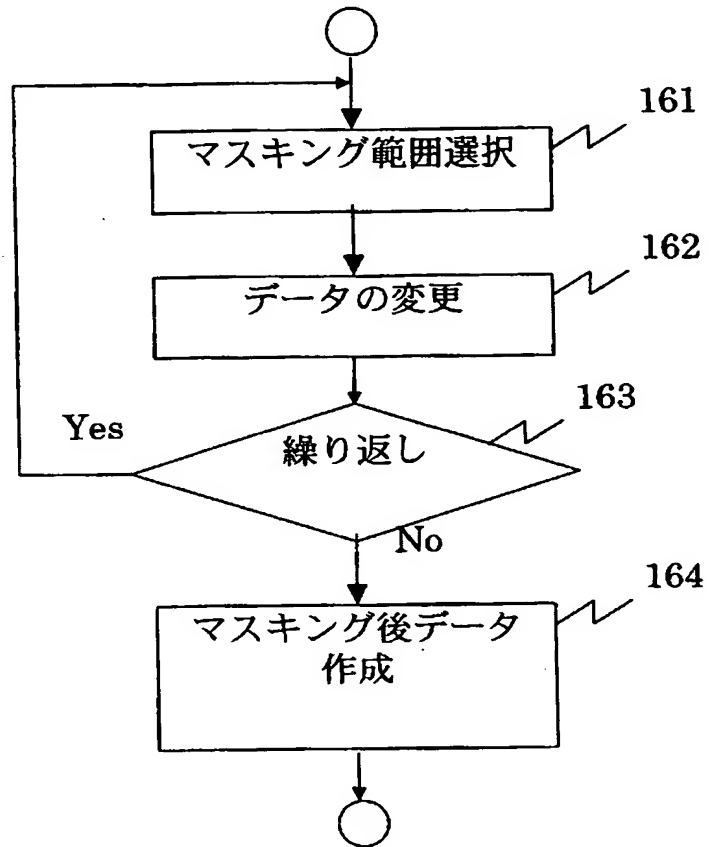
【図 8】

図 8



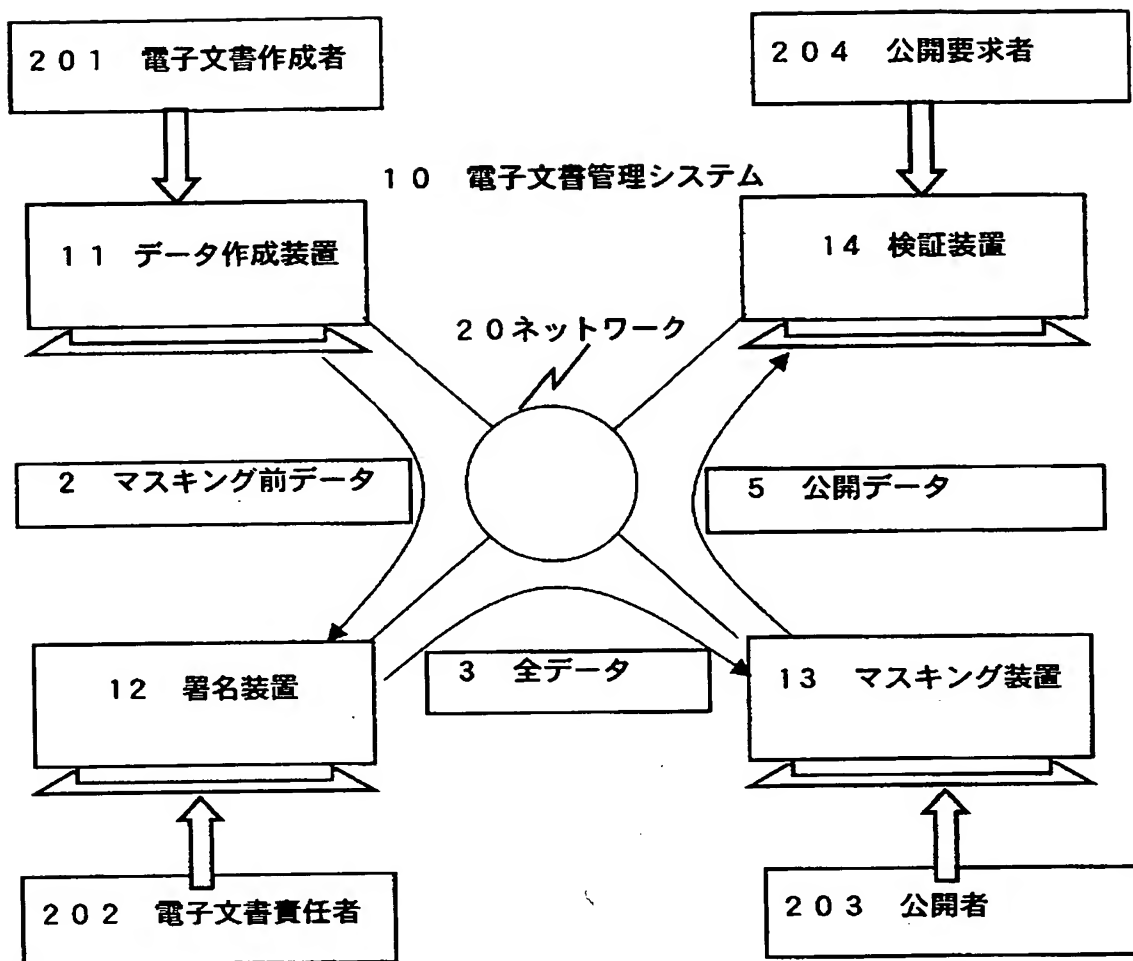
【図 9】

図 9



【図10】

図10



【書類名】 要約書

【要約】

【課題】 署名された電子文書を公開する際に、プライバシー情報や秘密情報など公開できない箇所を削除するなどの方法でマスキングを行うと、電子文書の署名が有効でなくなってしまう、電子文書の正当性を保証できない。

【解決手段】 対象となる電子文書をいくつかの部分に分割し、それぞれの部分に対してハッシュ値または署名値を求める。求めた複数のハッシュ値または署名値に対して署名を行うことで、署名の有効のままで元になる電子文書をマスキングすることができる。また、複数のハッシュ値または署名値を用いて、元の電子文書を検証することによってマスキングした箇所が確認できる。

【選択図】 図 1 0

認定・付加情報

特許出願の番号	特願 2 0 0 3 - 1 6 1 5 0 5
受付番号	5 0 3 0 0 9 4 8 8 2 7
書類名	特許願
担当官	第七担当上席 0 0 9 6
作成日	平成 1 5 年 6 月 9 日

< 認定情報・付加情報 >

【提出日】	平成 15 年 6 月 6 日
-------	-----------------

次頁無

特願 2 0 0 3 - 1 6 1 5 0 5

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 1 0 8]

1. 変更年月日

1 9 9 0 年 8 月 3 1 日

[変更理由]

新規登録

住 所

東京都千代田区神田駿河台 4 丁目 6 番地

氏 名

株式会社日立製作所